**WHAT IS CLAIMED IS:**

1. In a security system comprising a control panel and a plurality of security devices interconnected to the control panel over a communications medium located in a premises, a method of authenticating a security device to determine if it is authorized to be used with the security system, the method comprising the steps of:

a. storing a first encryption key and a second encryption key in the control panel;

b. storing the first encryption key and the second encryption key in the security device;

c. generating a challenge index at the control panel;

d. producing a challenge message by encrypting the challenge index using the first encryption key at the control panel and including the encrypted challenge index in the challenge message;

e. transmitting the challenge message over the communications medium to the security device;

f. receiving at the security device the challenge message over the communications medium from the control panel;

g. extracting the encrypted challenge index from the challenge message;

h. decrypting the encrypted challenge index using the first encryption key at the security device to produce a response index;

i. producing a response message by encrypting the response index using the second encryption key at the security device and including the encrypted response index in the response message;

j. transmitting the response message over the communications medium to the control panel;

k. receiving at the control panel the response message over the communications medium from the security device;

l. extracting the encrypted response index from the response message;

m. decrypting the encrypted response index using the second encryption key at the control panel to produce the response index;

n. comparing the response index decrypted by the control panel with the challenge index generated by the control panel;

   i. if the response index decrypted by the control panel is the same as the challenge index generated by the control panel, then indicating that the security device is authentic and allowing further communications between the control panel and the security device; and

   ii. if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then indicating that the security device is not authentic and disallowing further communications between the control panel and the security device.

2. The method of claim 1 wherein the method is performed during installation of the security device in the security system.

3. The method of claim 1 wherein the method is performed on a periodic basis during operation of the security system.

4. The method of claim 1 wherein, if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then sending a non-authentication message to a display device interconnected to the communications medium and displaying a message on the display device that indicates that authentication of the security device has failed.

5. The method of claim 1 wherein, if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then setting a flag in memory indicating that the authentication of the security device has failed.

6. The method of claim 1 wherein the index is a randomly generated number.

7. The method of claim 1 wherein the control panel and the security device communicate with each other via a gateway device.

8. In a security system comprising a control panel and a plurality of security devices interconnected to the control panel over a communications medium located in a premises, a method for a control panel to authenticate a security device to determine if it is authorized to be used with the security system, the method comprising the steps of:

a. storing a first encryption key and a second encryption key in the control panel;

b. generating a challenge index at the control panel;

c. producing a challenge message by encrypting the challenge index using the first encryption key at the control panel and including the encrypted challenge index in the challenge message;

d. transmitting the challenge message over the communications medium to the security device;

e. receiving at the control panel a response message over the communications medium from the security device;

f. extracting an encrypted response index from the response message;

g. decrypting the encrypted response index using the second encryption key at the control panel to produce the response index;

h. comparing the response index decrypted by the control panel with the challenge index generated by the control panel;

   i. if the response index decrypted by the control panel is the same as the challenge index generated by the control panel, then indicating that the security device is authentic and allowing further communications between the control panel and the security device; and

   ii. if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then indicating that the security device is not authentic and disallowing further communications between the control panel and the security device.

9. The method of claim 8 wherein the index is a randomly generated number.

10. In a security system comprising a control panel and a plurality of security devices interconnected to the control panel over a communications medium located in a premises, a method for a security device to respond to an authentication request to determine if it is authorized to be used with the security system, the method comprising the steps of:

a. storing a first encryption key and a second encryption key in the security device;

b. receiving at the security device a challenge message over the communications medium from the control panel;

c. extracting an encrypted challenge index from the challenge message;

d. decrypting the encrypted challenge index using the first encryption key at the security device to produce a response index;

e. producing a response message by encrypting the response index using the second encryption key at the security device and including the encrypted response index in the response message; and

f. transmitting the response message over the communications medium to the control panel.

11. The method of claim 10 wherein the index is a randomly generated number.

12. A security system comprising:

a. a control panel;

b. a plurality of security devices; and

c. a communications medium interconnecting the plurality of security devices with the control panel;

d. wherein the control panel comprises:

(i) a memory that stores a first encryption key and a second encryption key; and

(ii) processing circuitry adapted to:

(a) generate a challenge index;

(b) produce a challenge message by encrypting the challenge index using the first encryption key and including the encrypted challenge index in the challenge message; and

(c) transmit the challenge message over the communications medium to a security device being authenticated for use with the security system;

e. wherein the security device being authenticated for use with the security system comprises:

(i) a memory that stores the first encryption key and the second encryption key; and

(ii) processing circuitry adapted to:

(a) receive the challenge message over the communications medium from the control panel;

(b) extract the encrypted challenge index from the challenge message;

(c) decrypt the encrypted challenge index using the first encryption key stored at the security device to produce a response index;

(d) produce a response message by encrypting the response index using the second encryption key stored at the security device and including the encrypted response index in the response message; and

(e) transmit the response message over the communications medium to the control panel; and

f. wherein the processing circuitry at the control panel is further adapted to:

(i) receive the response message over the communications medium from the security device;

(ii) extract the encrypted response index from the response message;

(iii) decrypt the encrypted response index using the second encryption key stored at the control panel to produce the response index;

(iv) compare the response index decrypted by the control panel with the challenge index generated by the control panel; and

(a) if the response index decrypted by the control panel is the same as the challenge index generated by the control panel, then indicate that the security device is authentic and allow further communications between the control panel and the security device; and

(b) if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then indicate that the security device is not authentic and disallow further communications between the control panel and the security device.

13. The system of claim 12 wherein, if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, the processing circuitry at the control panel is further adapted

to set a flag in memory indicating that the authentication of the security device has failed.

14. The system of claim 12 further comprising a display device interconnected to the communications bus, and wherein, if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, the processing circuitry at the control panel is further adapted to send a non-authentication message to a display device interconnected to the communications bus, and wherein the display device is adapted to display a message that indicates that authentication of the security device has failed.

15. The system of claim 12 wherein the processing circuitry is adapted to generate a challenge index by generating a random number.

16. A control panel for use with a security system comprising:

a. a memory that stores a first encryption key and a second encryption key; and

b. processing circuitry adapted to:

(i) generate a challenge index;

(ii) produce a challenge message by encrypting the challenge index using the first encryption key and including the encrypted challenge index in the challenge message; and

(iii) transmit the challenge message over a communications medium to a security device being authenticated for use with the security system;

(iv) receive a response message over the communications medium from the security device;

(v) extract an encrypted response index from the response message;

(vi) decrypt the encrypted response index using the second encryption key stored at the control panel to produce the response index;

(vii) compare the decrypted response index with the generated challenge index generated; and

(a) if the response index decrypted by the control panel is the same as the challenge index generated by the control panel, then indicate that the security device is authentic and allow further communications between the control panel and the security device; and

(b) if the response index decrypted by the control panel is not the same as the challenge index generated by the control panel, then indicate that the security device is not authentic and disallow further communications between the control panel and the security device.

17. The control panel of claim 16 wherein the processing circuitry is adapted to generate a challenge index by generating a random number.

18. A security device for use with a security system comprising:

a. a memory that stores a first encryption key and a second encryption key; and

b. processing circuitry adapted to:

i. receive a challenge message over a communications medium from a control panel;

ii. extract an encrypted challenge index from the challenge message;

iii. decrypt the encrypted challenge index using the first encryption key stored at the security device to produce a response index;

iv. produce a response message by encrypting the response index using the second encryption key stored at the security device and including the encrypted response index in the response message; and

v. transmit the response message over the communications medium to the control panel.

19. The device of claim 18 wherein the index is a random number.

20. The security device of claim 18 further comprising a security sensor for detecting a change in condition in a surrounding environment.

21. The security device of claim 20 wherein the security sensor is a passive infrared motion detector.

22. The security device of claim 20 wherein the security sensor is a microwave motion detector.

23. The security device of claim 20 wherein the security sensor is a door opening sensor.

24. The security device of claim 20 wherein the security sensor is a glass breakage detector.

25. The security device of claim 20 wherein the security sensor is a smoke alarm.

26. The security device of claim 20 wherein the security sensor is a window opening detector.

27. The security device of claim 18 further comprising a security alarm sounder.

28. The security device of claim 18 further comprising a data entry device.

29. The security device of claim 18 further comprising a visual display.

30. The security device of claim 18 further comprising a dialer unit.

31. The security device of claim 18 further comprising an RF receiver.

32. The security device of claim 18 further comprising an RF transmitter.

33. The security device of claim 18 further comprising a bus gateway.

34. In a security system comprising a plurality of security devices interconnected over a communications medium located in a premises, wherein a first security device of said plurality of security devices is known to be authentic, a method of authenticating a second security device to

determine if it is authorized to be used with the security system, the method comprising the steps of:

a. storing a first encryption key and a second encryption key in the first security device;

b. storing the first encryption key and the second encryption key in the second security device;

c. generating a challenge index at the first security device;

d. producing a challenge message by encrypting the challenge index using the first encryption key at the first security device and including the encrypted challenge index in the challenge message;

e. transmitting the challenge message over the communications medium to the second security device;

f. receiving at the second security device the challenge message over the communications medium from the first security device;

g. extracting the encrypted challenge index from the challenge message;

h. decrypting the encrypted challenge index using the first encryption key at the second security device to produce a response index;

i. producing a response message by encrypting the response index using the second encryption key at the second security device and including the encrypted response index in the response message;

j. transmitting the response message over the communications medium to the first security device;

k. receiving at the first security device the response message over the communications medium from the second security device;

l. extracting the encrypted response index from the response message;

m. decrypting the encrypted response index using the second encryption key at the first security device to produce the response index;

n. comparing the response index decrypted by the first security device with the challenge index generated by the first security device;

i. if the response index decrypted by the first security device is the same as the challenge index generated by the first security device, then indicating that the second security device is authentic and allowing further communications between the first security device and the second security device; and

ii. if the response index decrypted by the first security device is not the same as the challenge index generated by the first security device, then indicating that the second security device is not authentic and disallowing further communications between the first security device and the second security device.

35. A security system comprising:

a. a plurality of security devices comprising a first security device known to be authentic and a second security device to be authenticated for use with the security system,; and

b. a communications medium interconnecting the plurality of security devices;

c. wherein the first security device comprises:

i. a memory that stores a first encryption key and a second encryption key; and

ii. processing circuitry adapted to:

(a) generate a challenge index;

(b) produce a challenge message by encrypting the challenge index using the first encryption key and including the encrypted challenge index in the challenge message; and

(c) transmit the challenge message over the communications medium to the second security device;

d. wherein the second security device comprises:

i. a memory that stores the first encryption key and the second encryption key; and

ii. processing circuitry adapted to:

(a) receive the challenge message over the communications medium from the first security device;

(b) extract the encrypted challenge index from the challenge message;

(c) decrypt the encrypted challenge index using the first encryption key stored at the second security device to produce a response index;

(d) produce a response message by encrypting the response index using the second encryption key stored at the second security device and including the encrypted response index in the response message; and

(e) transmit the response message over the communications medium to the first security device;

e. wherein the processing circuitry at the first security device is further adapted to:

i. receive the response message over the communications medium from the second security device;

ii. extract the encrypted response index from the response message;

iii. decrypt the encrypted response index using the second encryption key stored at the first security device to produce the response index;

iv. compare the response index decrypted by the first security device with the challenge index generated by the first security device; and

(a) if the response index decrypted by the first security device is the same as the challenge index generated by the first security device, then indicate that the second security device is authentic and allow further communications between the first security device and the second security device; and

(b) if the response index decrypted by the first security device is not the same as the challenge index generated by the first security device, then indicate that the second security device is not authentic and disallow further communications between the first security device and the second security device.